AF
SFW

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 10005248-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Mehrban Jam

Confirmation No.: 6956

Application No.: 09/836,952

Examiner: Fred I. Ehichioya

Filing Date: 04-17-2001

Group Art Unit: 2162

Title: System and Method for Providing Context-Aware Computer Management Using Smart Identification Badges

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on 10-30-2006.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☐ 1st Month $120	☐ 2nd Month $450	☐ 3rd Month $1020	☐ 4th Month $1590

☐ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of ~~$500~~ $60 ($440 WAS PREVIOUSLY PAID ON JUNE 8, 2004). At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

☒ A duplicate copy of this transmittal letter is enclosed.

☒ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:
Commissioner for Patents, Alexandria, VA 22313-1450
Date of Deposit: December 29, 2006

OR

☐ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571)273-8300.
Date of facsimile:
Typed Name: Ginger Yount
Signature: Ginger Yount

Respectfully submitted,
Mehrban Jam
By _____
Dan C. Hu
Attorney/Agent for Applicant(s)
Reg No. : 40,025
Date : December 29, 2006
Telephone : (713) 468-8880, ext. 304

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Mehrban Jam	§	Art Unit:	2162
		§		
Serial No.:	09/836,952	§		
		§	Examiner:	Fred I. Ehichioya
Filed:	April 17, 2001	§		
		§		
For:	System and Method for Providing Context-Aware Computer Management Using Smart Identification Badges	§	Atty. Dkt. No.:	10005248-1 (HPC.0209US)

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF PURSUANT TO 37 C.F.R § 41.37

Sir:

The final rejection of claims 1-38 is hereby appealed.

I. REAL PARTY IN INTEREST

The real party in interest is the Hewlett-Packard Development Company, L.P.

II. RELATED APPEALS AND INTERFERENCES

None.

III. STATUS OF THE CLAIMS

Claims 1-38 have been finally rejected and are the subject of this appeal.

Date of Deposit: December 29, 2006

I hereby certify under 37 CFR 1.8(a) that this correspondence is being deposited with the United States Postal Service as **first class mail** with sufficient postage on the date indicated above and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313.

Ginger Yount

Ginger Yount

IV. STATUS OF AMENDMENTS

No amendment after final has been submitted.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The following provides a concise explanation of the subject matter defined in each of the independent claims involved in the appeal, referring to the specification by page and line number and to the drawings by reference characters, as required by 37 C.F.R. § 41.37(c)(1)(v). Each element of the claims is identified by a corresponding reference to the specification and drawings where applicable. Note that the citation to passages in the specification and drawings for each claim element does not imply that the limitations from the specification and drawings should be read into the corresponding claim element.

Independent claim 1 recites a computer-implemented method comprising:

assigning information stored on a computer (Fig. 2:202) a plurality of clearance levels (Spec., 8:9-20);

assigning each smart badge (Fig. 2:210, 212, 214, 216) within a set of smart badges one of the clearance levels (Spec., 8:10-11);

using a wireless beacon (Fig. 2:206) to detect which smart badges are located within a predefined boundary (Spec., 8:5-8);

identifying a lowest clearance level assigned to the smart badges within the boundary (Spec., 9:16-10:12); and

providing access to that sub-set of the information having a clearance level no higher than the lowest identified clearance level (Spec., 9:16-10:12).

Independent claim 12 recites a method for context-aware computer management comprising:

> assigning database information a plurality of clearance levels (Spec., 8:9-20);
>
> assigning each smart badge within a set of smart badges one of the clearance levels (Spec., 8:10-11);
>
> using a wireless beacon (Fig. 2:206) to detect which smart badges are located within a predefined physical boundary (Spec., 8:5-8);
>
> identifying a lowest clearance level assigned to the smart badges within the boundary (Spec., 9:16-10:12);
>
> providing access to that sub-set of the database information having a clearance level no higher than the lowest identified clearance level on a computer located within the predefined physical boundary (Spec., 9:16-10:12);
>
> defining those smart badges within the boundary as a set of visible smart badges (Spec., 11:5-7);
>
> updating the set of visible smart badges in response to a change in smart badge visibility status (Spec., 11:8-13:4); and
>
> recalculating the lowest clearance level in response to the change in smart badge visibility status (Spec., 9:16-10:12).

Independent claim 13 recites a computer-usable medium embodying computer program code for context-aware computer management, comprising:

> assigning database information a plurality of clearance levels (Spec., 8:9-20);
>
> assigning each smart badge within a set of smart badges one of the clearance levels (Spec., 8:10-11);
>
> using a wireless beacon (Fig. 2:206) to detect which smart badges are located within a predefined physical boundary (Spec., 8:5-8);
>
> identifying a lowest clearance level assigned to the smart badges within the boundary (Spec., 9:16-10:12); and
>
> providing access to that sub-set of the database information having a clearance level no higher than the lowest identified clearance level on a computer located within the predefined physical boundary (Spec., 9:16-10:12).

Independent claim 20 recites a system for context-aware computer management comprising:

means for assigning database information a plurality of clearance levels (Spec., 8:9-20);

means for assigning each smart badge within a set of smart badges one of the clearance levels (Spec., 8:10-11);

means for using a wireless beacon (Fig. 2:206) to detect which smart badges are located within a predefined physical boundary (Spec., 8:5-8);

means for identifying a lowest clearance level assigned to the smart badges within the boundary (Spec., 9:16-10:12);

means for providing access to that sub-set of the database information having a clearance level no higher than the lowest identified clearance level on a computer located within the predefined physical boundary (Spec., 9:16-10:12);

means for defining those smart badges within the boundary as a set of visible smart badges (Spec., 11:5-7);

means for updating the set of visible smart badges in response to a change in smart badge visibility status (Spec., 11:8-13:4); and

means for recalculating the lowest clearance level in response to the change in smart badge visibility status (Spec., 9:16-10:12).

Independent claim 21 recites a system for context-aware computer management comprising:

a database (Fig. 2:208), including information differentiated by a plurality of clearance levels (Spec., 8:9-20);

a first wireless beacon (Fig. 2:206);

a set of smart badges (Fig. 2:210, 212, 214, 216), detected by the first wireless beacon to be within a predefined boundary, each badge assigned one of the clearance levels (Spec., 8:5-8, 10-11);

a computer (Fig. 2:202) located within the boundary (Spec., 7:3-7);

a system service module (Fig. 2:218), coupled to the first wireless beacon, for identifying a lowest clearance level assigned to the smart badges within the boundary (Spec., 9:6-10:12); and

a software application (Fig. 2:222), coupled to the system service module and the database, for providing access to that sub-set of the information within the database having a clearance level no higher than the lowest identified clearance level on the computer (Spec., 9:6-10:12).

Independent claim 31 recites an article comprising a computer-usable medium containing program code that when executed cause a computer to:

store plural sub-sets of information, each sub-set of information associated with one of plural clearance levels (Spec., 8:9-20);

use at least a first wireless beacon (Fig. 2:206) to communicate with plural badges (Fig. 2:210, 212, 214, 216) within a predefined region, each of the plural badges associated with one of the plural clearance levels (Spec., 8:5-8);

determine a lowest clearance level from among the clearance levels associated with the badges in the predefined region (Spec., 9:16-10:12); and

provide access to one or more sub-sets of the information having one or more respective clearance levels no higher than the determined lowest clearance level (Spec., 9:16-10:12).

Independent claim 36 recites a system comprising:

storage to store sub-sets of information associated with corresponding plural clearance levels (Spec., 8:9-20);

a first wireless beacon (Fig. 2:206) to communicate wirelessly with badges (Fig. 2:210, 212, 214, 216) within a predefined region, each of the badges associated with one of the plural clearance levels (Spec., 8:5-8);

a module (Fig. 2:218) to identify a lowest clearance level from among the clearance levels of the badges within the predefined region (Spec., 9:6-10:12); and

software (Fig. 2:222) to provide access to one or more sub-sets of information in the storage having one or more clearance levels no higher than the identified lowest clearance level (Spec., 9:6-10:12).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Claims 1-8, 10-17, 19-21, And 24-27 Rejected Under 35 U.S.C. § 103 Over "Accessing The Campus," By Joe Gallagher ("Gallagher") In View Of "Smart Card Policy And Administrative Guidelines," By General Services Administration ("GSA").

B. Claims 9 And 18 Rejected Under 35 U.S.C. § 103 Over Gallagher In View Of GSA And U.S. Patent No. 6,057,764 (Williams).

C. Claims 22, 23, And 28-30 Rejected Under 35 U.S.C. § 103 Over Gallagher In View Of GSA And U.S. Patent No. 6,633,757 (Hermann).

D. Claims 31-33, And 35-38 Rejected Under 35 U.S.C. § 103 Over GSA In View Of Hermann.

E. Claim 34 Rejected Under 35 U.S.C. § 103 Over GSA In View Of Hermann And Williams.

VII. ARGUMENT

The claims do not stand or fall together. Instead, Appellant presents separate arguments for various independent and dependent claims. Each of these arguments is separately argued below and presented with separate headings and sub-headings as required by 37 C.F.R. § 41.37(c)(1)(vii).

A. Claims 1-8, 10-17, 19-21, And 24-27 Rejected Under 35 U.S.C. § 103 Over "Accessing The Campus," By Joe Gallagher ("Gallagher") In View Of "Smart Card Policy And Administrative Guidelines," By General Services Administration ("GSA").

1. Claims 1, 5, 7, 13, and 16.

Independent claim 1 was rejected as allegedly being obvious over Gallagher and GSA. It is respectfully submitted that a *prima facie* case of obviousness has not been established with respect to claim 1 over Gallagher and GSA for at least the following reasons: (1) no motivation or suggestion existed to combine the teachings of Gallagher and GSA; and (2) the references

when combined do not teach or suggest *all* elements of the claim. M.P.E.P. § 2143 (8th ed., Rev. 5), at 2100-126.

Claim 1 recites a method that includes the following acts:

- assigning information stored on a computer a plurality of clearance levels;
- assigning each smart badge within a set of smart badges one of the clearance levels;
- using a *wireless beacon to detect* which smart badges are located *within a predefined boundary*;
- identifying a *lowest clearance level* assigned to *the* smart badges *within the boundary*; and
- providing access to that sub-set of the information having a clearance level no higher than the lowest identified clearance level.

The Examiner conceded that Gallagher does not disclose the identifying and providing acts of claim 1. 1/27/2006 Office Action at 4. The Examiner relied instead on GSA as disclosing these two elements. *Id.*

It is respectfully submitted that the Examiner has incorrectly asserted that GSA discloses the identifying and providing acts of claim 1. Note that claim 1 recites identifying a lowest clearance level assigned to *the* smart badges *within a boundary*. "The" smart badges refer to the smart badges detected to be located within the predefined boundary by the wireless beacon. The Examiner cited page 114 of GSA as disclosing such identifying. Page 114 and the subsequent pages after page 114 of GSA refer to various agency profile models that can be used. The model referred to on page 114 of GSA is the small agency model, in which a low level security is employed for a small agency, such as a small division or bureau of a larger agency, or a particular facility within a large organization. Other agency profile models are described in the remaining parts of GSA.

The term "lowest level security" mentioned on page 114 of GSA refers to the security needs of a small agency model. Due to the relatively small size of the small agency, the security needs are low. Page 117 of GSA refers to a campus/metro area agency model that has a higher level security need, followed by a civilian agency model (page 120 of GSA), a commercial agency model (page 125 of GSA), and so forth. There is absolutely no teaching or suggestion whatsoever in GSA of identifying a lowest clearance level assigned to the smart badges *within a boundary*, where the smart badges are the smart badges detected to be within the predefined boundary by the wireless beacon.

In making the obviousness rejection, the Examiner appears to have ignored explicit elements recited in the claims, and to have applied the teachings of GSA out of context. With respect to page 114 of GSA, the Examiner contended that "GSA discloses 'this model has the lowest level security needs which the examiner interprets as identifying a lowest clearance level.'" 7/28/2006 Office Action at 2. The Examiner further contended that "GSA also discloses in this section 'Employee cards are to be used in a single geographic location,'" which the Examiner interpreted as being the predefined boundary recited in claim 1. In making the assertions above, the Examiner has ignored specific words of the claim, and the relationship between different elements of claim 1. Read in proper context, page 114 of GSA teaches that for the Small Agency Model, where the security needs are low, employee cards are to be used in a single geographic location. In contrast, the elements at issue in claim 1 refer to identifying a lowest clearance level assigned to *the* smart badges within the boundary, where *the* smart badges are those detected to be located within the predefined boundary using a wireless beacon. There is clearly absolutely no suggestion whatsoever by GSA of this feature of claim 1.

Thus, in performing the obviousness analysis, the Examiner has taken words from the claims out of context, and then applied such words to the teachings of GSA. Such an obviousness analysis is clearly improper. The teachings of a reference must be considered in its entirety, as must the elements of a claim. Claim elements in one clause of a claim must be considered in relation to other clauses in the claim, particularly where there is a specific relationship recited in the claim. In this case, the using act and identifying act of claim 1 are clearly interrelated by "the smart badges within the boundary," and this relationship cannot be ignored when making the obviousness analysis. In view of the fact that the hypothetical combination of Gallagher and GSA does not teach or suggest all elements of claim 1, the Examiner has failed to establish a *prima facie* case of obviousness with respect to the claim for at least this reason.

Also, a further defect of the obviousness rejection is that no motivation or suggestion existed to combine the teachings of Gallagher and GSA to achieve the claimed subject matter. Gallagher describes cards used by students to access different parts of a school campus. GSA describes using smart cards for building access control (to access a physical location such as a building, office, etc.) and logical access control (to control access of computer system resources). GSA, p. 5. However, GSA does not provide any suggestion to modify Gallagher to achieve the claimed subject matter. Neither Gallagher nor GSA even remotely suggests the desirability of modifying their mechanisms to enable the detection of smart badges within a predefined boundary and identifying a lowest clearance level assigned to the smart badges within the predefined boundary such that access to that sub-set of information having a clearance level no higher than the lowest identified clearance level is provided. *See In re Fritch*, 972 F.2d 1260, 1266, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992) ("The mere fact that the prior art may be modified in

the manner suggested by the Examiner does not make the modification obvious unless the prior art suggested the desirability of the modification.").

The Examiner argued that the "motivation to combine the cited references is that the combined system will provide a standardized card which could be read interoperably by multiple types of readers[, where this] interoperability makes it easy to check unauthorized access." 7/28/2006 Office Action at 3. This stated motivation by the Examiner, even if true, is clearly unrelated to the subject matter of claim 1. The key issue is whether a person of ordinary skill in the art would have combined the teachings of Gallagher and GSA to achieve the claimed subject matter. In this case, Gallagher teaches cards that are used by students that access different parts of a school campus, whereas GSA states that different security models can be used for different levels of security needs. There is no teaching, explicit or implicit, in either Gallagher or GSA of modifying the Gallagher system to incorporate the ability to use a wireless beacon to detect which smart badges are located within a predefined boundary, identifying a lowest clearance level assigned to the smart badges within the boundary, and providing access to that sub-set of the information having a clearance level no higher than the lowest identified clearance level. Therefore, since no motivation or suggestion existed to combine the teachings of Gallagher and GSA, the *prima facie* case of obviousness is defective.

Independent claim 13 is allowable for at least the same reasons as claim 1. Dependent claims of claims 1 and 13 are allowable for at least the same reasons as corresponding independent claims. Reversal of the final rejection of the above claims is respectfully requested.

2. Claims 2, 4, and 14.

Claims 2, 4, and 14 depend from claims 1 and 13, respectively, and are thus allowable for at least the same reasons. Moreover, claim 2 recites defining those smart badges within the boundary as a set of visible smart badges, and updating the set of visible smart badges in response to a change in smart badge visibility status. The Examiner cited page 2 of Gallagher, and ¶¶ 1 and 2, as disclosing this feature of claim 2. Paragraphs 1 and 2 on page 2 of Gallagher describe a one-card system that includes a photo-imaging system to allow a campus to design a number of different types of cards for day students, night students, residents, employees, and volunteers. The cited passages also state that campuses can use the one-card system for registration, where the cards can be activated and deactivated easily according to a student's status. The cited passages of Gallagher state that if a student drops out mid-semester, the card can be deactivated. There is absolutely nothing in these cited passages of Gallagher to even remotely suggest defining those smart badges within the boundary as a set of visible smart badges, and updating the set of visible smart badges in response to a change in smart badge visibility status. Therefore, each of claims 2, 4, and 14 is further allowable for the foregoing reasons.

Reversal of the final rejection of the above claims is respectfully requested.

3. Claims 3 and 15.

Claims 3 and 15 depend from claims 2 and 14, respectively, and are thus allowable for at least the same reasons as those base claims. Moreover, claim 3 recites recalculating the lowest clearance level in response to the change in smart badge visibility status. The Examiner cited page 4, ¶ 5, of Gallagher as disclosing this feature. The cited passage of Gallagher refers to a one-card system that provides security for certain areas of the campus, with magnetic-card

readers allowing the card to be used as an electronic key, and where access can be tailored for each individual card. There is no mention or suggestion in this passage of Gallagher, or anywhere else in Gallagher, of recalculating the lowest clearance level in response to a change in smart badge visibility status.

Therefore, reversal of the final rejection of the above claims is respectfully requested for these additional reasons.

4. Claims 6 and 17.

Claims 6 and 17 depend from claims 2 and 14, respectively, and are thus allowable for similar reasons as respective base claims. Moreover, claim 6 recites preventing access to the information when the smart badge visibility status is set to *invisible for a predetermined timeout.* The Examiner cited page 1, ¶ 4, of Gallagher as disclosing this feature. The cited passage of Gallagher refers to magnetic-card readers to allow cardholders to use the card as an electronic key, with access tailored to each individual, and which access can be terminated or updated quickly, without retrieval of the card. However, nowhere in this passage of Gallagher is there any suggestion of preventing access to information when the smart badge *visibility* status is set to *invisible for a predetermined timeout.*

In view of the foregoing additional reasons, reversal of the final rejection of the above claims is respectfully requested.

5. Claim 8.

Claim 8 depends indirectly from claim 1, and is thus allowable for at least the same reasons. Moreover, claim 8 recites pre-reading data items from the smart badges during *idle periods*. The Examiner cited page 16 of GSA, and in particular, the "serial protected memory

integrated chip cards" of GSA, as disclosing this feature of claim 8. The cited passage of GSA refers to protected memory cards implemented as prepaid disposable cards that use read/write memory and binary counting schemes that allow the cards to carry more than 20,000 units of value. However, nowhere in this cited passage of GSA is there any suggestion of pre-reading data items from smart badges *during idle periods*, as recited in claim 8. For the foregoing additional reasons, reversal of the final rejection of the above claim is respectfully requested.

6. Claims 10 and 19.

Claims 10 and 19 depend from claims 1 and 13, respectively, and are thus allowable for at least the same reasons as corresponding independent claims. Moreover, claim 10 recites assigning an expiration period to each of the smart badges, and de-authenticating and erasing all data stored on a smart badge whose expiration period has been exceeded. The Examiner cited page 2, ¶ 2, of Gallagher as disclosing the features of claims 10 and 19. The Examiner stated that "activate or deactivate" is equivalent to "assigning an expiration period to each of the smart badges." 7/28/2006 Office Action at 9. The activation and deactivation referred to in the cited passage of Gallagher refers to activating and deactivating cards according to a student's status. However, nowhere is there any suggestion of assigning an *expiration period* to each of the smart badges. Also, deactivating a card of a student that drops out at mid-semester, as taught by Gallagher in the cited passage, is not the same as de-authenticating and erasing all data stored on a smart badge whose *expiration period has been exceeded.*

For the foregoing additional reasons, reversal of the final rejection of the above claims is respectfully requested.

7. Claim 11.

Claim 11 depends from claim 1, and is thus allowable for at least the same reasons as claim 1. Moreover, claim 11 recites configuring the predefined boundary by varying a sensitivity level of the wireless beacon. The Examiner cited page 62, § 1, ¶ 1, of GSA as disclosing this feature. The cited passage refers to different government agencies and departments having different security needs. Nowhere in this cited passage of GSA is there any suggestion of configuring a pre-defined boundary by *varying a sensitivity level of the wireless beacon.*

For the foregoing additional reasons, reversal of the final rejection of the above claim is respectfully requested.

8. Claim 27.

Claim 27 depends from claim 1, and is thus allowable for at least the same reasons. Moreover, claim 27 recites providing access to the sub-set of information *stored on the computer located within the predefined boundary.* The Examiner cited page 78 of GSA as disclosing this feature. Page 78 of GSA refers to agencies having low level security needs in which pass codes can be used for security. Page 78 of GSA also mentions that agencies that have higher level security needs can consider a chip card to enable use of biometric, digital certificate, or card-based pass code for system access. Nowhere on page 78 of GSA is there any hint or suggestion of providing access to the sub-set of information stored on *the computer located within the predefined boundary*, which is the same predefined boundary in which smart badges are detected to be located using a wireless beacon.

For the foregoing additional reasons, reversal of the final rejection of the above claim is respectfully requested.

9. Claims 12 and 20.

Independent claim 12 was also rejected as being obvious over Gallagher and GSA. Claim 12 recites using a wireless beacon to detect which smart badges are located within a predefined physical boundary, identifying a lowest clearance level assigned to the smart badges within the predefined physical boundary, and providing access to that sub-set of the database information having a clearance level no higher than the lowest identified clearance level on a computer located within the predefined physical boundary. As discussed above, there did not exist any motivation or suggestion to combine the teachings of Gallagher and GSA. Moreover, the hypothetical combination of Gallagher and GSA fails to teach or suggest using a wireless beacon to detect which smart badges are located within a predefined *physical boundary*, identifying a lowest clearance level assigned to the smart badges within the predefined physical boundary, and providing access to the sub-set of the database information having a clearance level no higher than the lowest identified clearance level on a computer located within the predefined physical boundary.

Claim 12 further recites defining those smart badges within the boundary as a set of visible smart badges, updating the set of visible smart badges in response to a change in smart badge visibility status, and recalculating the lowest clearance level in response to the change in smart badge visibility status. The Examiner cited page 2, ¶ 2, of Gallagher as disclosing the updating act of claim 12. The cited passage of Gallagher refers to activating and deactivating a card based on a student's status. There is no suggestion in this passage of updating the set of visible smart badges in response to a change in the smart badge visibility status, where the visible smart badges are those smart badges within the predefined physical boundary. Also, with respect to the recalculating act of claim 12, the Examiner cited page 4, ¶ 5, of Gallagher. The

cited passage on page 4 of Gallagher refers to magnetic-card readers that allow the card to be used as an electronic key, where access can be tailored for each individual card. There is no teaching or suggestion here of recalculating the lowest clearance level in response to the change in smart badge visibility status.

In view of the foregoing, it is respectfully submitted that a *prima facie* case of obviousness has not been established with respect to claim 12.

Independent claim 20 is similarly allowable.

In view of the foregoing, reversal of the final rejection of the above claims is respectfully requested.

10. Claims 21, 24, and 26.

With respect to independent claim 21, the asserted combination of Gallagher and GSA does not teach or suggest the following combination of elements: a set of smart badges, detected by the first wireless beacon to be within a predefined boundary, where each badge is assigned one of the plurality of clearance levels; a system service module, coupled to the first wireless beacon, for identifying a lowest clearance level assigned to the smart badges within the boundary; and a software application, for providing access to that sub-set of the information within the database having a clearance level no higher than the lowest identified clearance level on the computer.

As noted above, no motivation or suggestion existed to combine the teachings of Gallagher and GSA. Moreover, the hypothetical combination of Gallagher and GSA does not teach or suggest the combination of elements recited above.

In view of the foregoing, reversal of the final rejection of the above claims is respectfully requested.

11. Claims 25.

Claim 25 depends from claim 21, and is thus allowable for at least the same reasons as claim 21. Moreover, claim 25 recites that the service module defines those smart badges within the boundary as a set of visible smart badges, and recalculates the lowest clearance level in response to a change in the visibility status. As explained above in connection with claims 2 and 3 (§§ VII.A.2 and VII.A.3), the hypothetical combination of Gallagher and GSA does not disclose or suggest these features of claim 25. For the foregoing additional reasons, reversal of the final rejection of the above claim is respectfully requested.

B. Claims 9 And 18 Rejected Under 35 U.S.C. § 103 Over Gallagher In View Of GSA And U.S. Patent No. 6,057,764 (Williams).

1. Claims 9 and 18.

Claims 9 and 18 were rejected as being obvious over Gallagher, GSA, and Williams. In view of the fact that the obviousness rejection of base claims 1 and 13 is defective, it is respectfully submitted that the obviousness rejection of claims 9 and 18 over Gallagher, GSA, and Williams is also defective.

Moreover, with respect to claim 9, the Examiner conceded that Gallagher and GSA do not disclose defining a badge removal confidence level indicating whether each smart badge has been continuously worn by corresponding assigned smart badge wearers. Instead, the Examiner cited Williams, and in particular to column 6, lines 2-18, of Williams as disclosing this feature. The cited passage of Williams refers to a computer searching among authorized identification numbers for a particular space, or searching authorized identification numbers to determine if the identification number in question has a tag indicating authority to be within the particular space. The cited passage of Williams also notes that each badge can receive a cryptographic code upon

entry of the building, concomitant with visual recognition of the employee. Also, the cited passage of Williams notes that each triggering of a presence detector of an alarm system will cause an inquiry to determine if the person who set it off has a badge capable of responding with an identity number, and whether that identity number matches those that are permitted access to the particular space monitored by the presence detector. This teaching does not provide any suggestion of defining a badge *removal* confidence level indicating whether each smart badge has been *continuously worn* by corresponding assigned smart badge wearers.

In view of the foregoing reasons, reversal of the final rejection of the above claims is respectfully requested.

C. Claims 22, 23, And 28-30 Rejected Under 35 U.S.C. § 103 Over Gallagher In View Of GSA And U.S. Patent No. 6,633,757 (Hermann).

1. Claims 22, 23, and 28-30.

In view of the defective obviousness rejection of base claims 1 and 21 over Gallagher and GSA, it is respectfully submitted that the obviousness rejection of dependent claims 22, 23, and 28-30 over Gallagher, GSA, and Hermann is defective. Therefore, reversal of the final rejection of the above claims is respectfully requested.

D. Claims 31-33, And 35-38 Rejected Under 35 U.S.C. § 103 Over GSA In View Of Hermann.

1. Claims 31, 32, 35, and 36.

Independent claim 31 was rejected as being obvious over GSA in view of Hermann. As discussed above with respect to the other claims, it is respectfully submitted that the Examiner incorrectly stated that GSA discloses determining a lowest clearance level from among the clearance levels associated with a badges in a predefined region. Based at least on this

mis-application of GSA to claim 31, it is respectfully submitted that the obviousness rejection of claim 31 over GSA and Hermann is defective.

The Examiner conceded GSA does not disclose a first wireless beacon as recited in claim 31. 7/28/2006 Office Action at 17. However, the Examiner relied upon Hermann as disclosing this feature, citing specifically to column 12, lines 50-67, and column 6, lines 52-61, of Hermann. Although Hermann does disclose the use of an IR location beacon or an RF beacon, there is no suggestion within Hermann of modifying GSA to achieve the claimed subject matter, namely to use at least a first wireless beacon to communicate with plural badges within a predefined region, each of the plural badges associated with one of plural clearance levels, and determining a lowest clearance level from among the clearance levels associated with the badges in the predefined region. Therefore, it is respectfully submitted that the hypothetical combination of GSA and Hermann does not teach or suggest all elements of claim 31.

It is also respectfully submitted that no motivation or suggestion existed to combine the teachings of GSA and Hermann to achieve the claimed subject matter. As noted above, GSA fails to disclose the determining act of claim 31. Hermann clearly does not provide any suggestion of a modification of GSA to achieve that claimed elements. Therefore, because no motivation or suggestion existed to combine the teachings of GSA and Hermann, the *prima facie* case of obviousness of claim 31 is defective.

Independent claim 36 is allowable over GSA and Hermann for similar reasons as claim 31.

Reversal of the final rejections of the above claims is respectfully requested.

2. Claims 33, 37, and 38.

Claims 33, 37, and 38 depend from claims 31 and 36, respectively, and are thus allowable for at least the same reasons as corresponding independent claims. Moreover, claim 33 recites using a second wireless beacon to communicate with the plural badges in the predefined region and to communicate with one or more badges outside the predefined region, where the first wireless beacon is able to communicate with the plural badges within the predefined region, but is unable to communicate with the one or more badges outside the predefined region, and the badges are determined to be within the predefined region based on the first and second wireless beacons. The Examiner cited column 12 of Hermann as disclosing the subject matter of claim 33. Although column 12 of Hermann discloses an IR location beacon and an RF location beacon, there is no suggestion by Hermann of using first and second wireless beacons to enable the determination of whether badges are within a predefined region, as recited in the claims.

In view of the foregoing additional reasons, reversal of the final rejection of the above claims is respectfully requested.

E. Claim 34 Rejected Under 35 U.S.C. § 103 Over GSA In View Of Hermann And Williams.

1. Claim 34.

Claim 34 depends from claim 31. Claim 34 was rejected as being obvious over GSA, Hermann, and Williams. In view of the defective obviousness rejection of claim 31 over GSA and Hermann, it is respectfully submitted that the obviousness rejection of claim 34 over GSA, Hermann, and Williams is also defective.

In view of the foregoing, reversal of the final rejection of the above claim is respectfully requested.

VIII. CONCLUSION

In view of the foregoing, reversal of all final rejections and allowance of all pending claims is respectfully requested.

Respectfully submitted,

Date: Dec 29, 2006

Dan C. Hu
Registration No. 40,025
TROP, PRUNER & HU, P.C.
1616 South Voss Road, Suite 750
Houston, TX 77057-2631
Telephone: (713) 468-8880
Facsimile: (713) 468-8883

APPENDIX OF APPEALED CLAIMS

The claims on appeal are:

1. A computer-implemented method comprising:

assigning information stored on a computer a plurality of clearance levels;

assigning each smart badge within a set of smart badges one of the clearance levels;

using a wireless beacon to detect which smart badges are located within a predefined boundary;

identifying a lowest clearance level assigned to the smart badges within the boundary; and

providing access to that sub-set of the information having a clearance level no higher than the lowest identified clearance level.

2. The method of claim 1 further comprising:

defining those smart badges within the boundary as a set of visible smart badges; and

updating the set of visible smart badges in response to a change in smart badge visibility status.

3. The method of claim 2 further comprising:

recalculating the lowest clearance level in response to the change in smart badge visibility status.

4. The method of claim 2 further comprising:

recording the smart badge visibility status of each smart badge within an activity log.

5. The method of claim 1 wherein providing includes:

providing access to smart badge wearers assigned to the smart badges.

6. The method of claim 2 further comprising:

preventing access to the information when the smart badge visibility status is set to invisible for a predetermined timeout.

7. The method of claim 1 further comprising:

writing data items to the smart badges.

8. The method of claim 7 further comprising:

pre-reading the data items from the smart badges during idle periods.

9. The method of claim 1 further comprising

defining a badge removal confidence level indicating whether each smart badge has been continuously worn by corresponding assigned smart badge wearers.

10. The method of claim 1 further comprising:

assigning an expiration period to each of the smart badges; and

de-authenticating and erasing all data stored on a smart badge whose expiration period has been exceeded.

11. The method of claim 1 wherein the using element includes:

configuring the predefined boundary by varying a sensitivity level of the wireless beacon.

12. A method for context-aware computer management comprising:

assigning database information a plurality of clearance levels;

assigning each smart badge within a set of smart badges one of the clearance levels;

using a wireless beacon to detect which smart badges are located within a predefined physical boundary;

identifying a lowest clearance level assigned to the smart badges within the boundary;

providing access to that sub-set of the database information having a clearance level no higher than the lowest identified clearance level on a computer located within the predefined physical boundary;

defining those smart badges within the boundary as a set of visible smart badges;

updating the set of visible smart badges in response to a change in smart badge visibility status; and

recalculating the lowest clearance level in response to the change in smart badge visibility status.

13. A computer-usable medium embodying computer program code for context-aware computer management, comprising:

assigning database information a plurality of clearance levels;

assigning each smart badge within a set of smart badges one of the clearance levels;

using a wireless beacon to detect which smart badges are located within a predefined physical boundary;

identifying a lowest clearance level assigned to the smart badges within the boundary; and

providing access to that sub-set of the database information having a clearance level no higher than the lowest identified clearance level on a computer located within the predefined physical boundary.

14. The computer-usable medium of claim 13 further comprising:

defining those smart badges within the boundary as a set of visible smart badges; and

updating the set of visible smart badges in response to a change in smart badge visibility status.

15. The computer-usable medium of claim 14 further comprising:

recalculating the lowest clearance level in response to the change in smart badge visibility status.

16. The computer-usable medium of claim 13 wherein providing includes:

providing access to the database information to smart badge wearers assigned to the smart badges.

17. The computer-usable medium of claim 14 further comprising:

preventing access to the database when the smart badge visibility status is set to invisible for a predetermined timeout.

18. The computer-usable medium of claim 13 further comprising

defining a badge removal confidence level indicating whether each smart badge has been continuously worn by corresponding assigned smart badge wearers.

19. The computer-usable medium of claim 13 further comprising:

assigning an expiration period to each of the smart badges; and

de-authenticating and erasing all data stored on a smart badge whose expiration period has been exceeded.

20. A system for context-aware computer management comprising:

means for assigning database information a plurality of clearance levels;

means for assigning each smart badge within a set of smart badges one of the clearance levels;

means for using a wireless beacon to detect which smart badges are located within a predefined physical boundary;

means for identifying a lowest clearance level assigned to the smart badges within the boundary;

means for providing access to that sub-set of the database information having a clearance level no higher than the lowest identified clearance level on a computer located within the predefined physical boundary;

means for defining those smart badges within the boundary as a set of visible smart badges;

means for updating the set of visible smart badges in response to a change in smart badge visibility status; and

means for recalculating the lowest clearance level in response to the change in smart badge visibility status.

21. A system for context-aware computer management comprising:

a database, including information differentiated by a plurality of clearance levels;

a first wireless beacon;

a set of smart badges, detected by the first wireless beacon to be within a predefined boundary, each badge assigned one of the clearance levels;

a computer located within the boundary;

a system service module, coupled to the first wireless beacon, for identifying a lowest clearance level assigned to the smart badges within the boundary; and

a software application, coupled to the system service module and the database, for providing access to that sub-set of the information within the database having a clearance level no higher than the lowest identified clearance level on the computer.

22. The system of claim 21, wherein the first beacon includes:
a wide angle RF beacon.

23. The system of claim 21, further comprising:
a second diffuse IR beacon, coupled to the service module, limited to detecting smart badges within the predefined boundary.

24. The system of claim 21, wherein the smart badges include:
biometric sensors for detecting when a smart badge has been removed from an assigned smart badge wearer.

25. The system of claim 21, wherein the service module
defines those smart badges within the boundary as a set of visible smart badges, and
recalculates the lowest clearance level in response to a change in a visibility status.

26. The system of claim 21, wherein the application logs smart badge wearers assigned to visible smart badges onto the computer.

27. The method of claim 1, wherein providing access to the sub-set of information comprises providing access to the sub-set of information stored on the computer located within the predefined boundary.

28. The method of claim 1, wherein the wireless beacon comprises a first wireless beacon to communicate with the smart badges, the method further comprising:
using a second wireless beacon to communicate with the smart badges,
wherein detecting which smart badges are located within the predefined boundary is based on the first and second wireless beacons.

29. The method of claim 28, wherein using the second wireless beacon comprises using the second wireless beacon to communicate with smart badges within the predefined boundary and to communicate with smart badges outside the predefined boundary through one or more blocking objects defining the predefined boundary, and

using the first wireless beacon comprises using the first wireless beacon to communicate with smart badges within the predefined boundary, wherein the first wireless beacon is blocked from communicating with smart badges outside the predefined boundary by the one or more blocking objects.

30. The method of claim 29, wherein using the first wireless beacon comprises using an infrared beacon, and wherein using the second wireless beacon comprises using a radio frequency beacon.

31. An article comprising a computer-usable medium containing program code that when executed cause a computer to:

store plural sub-sets of information, each sub-set of information associated with one of plural clearance levels;

use at least a first wireless beacon to communicate with plural badges within a predefined region, each of the plural badges associated with one of the plural clearance levels;

determine a lowest clearance level from among the clearance levels associated with the badges in the predefined region; and

provide access to one or more sub-sets of the information having one or more respective clearance levels no higher than the determined lowest clearance level.

32. The article of claim 31, wherein providing access to the one or more sub-sets of the information comprises displaying the one or more sub-sets of the information having the one or more respective clearance levels no higher than the determined lowest clearance level.

33. The article of claim 31, wherein the program code when executed cause the computer to further:

use a second wireless beacon to communicate with the plural badges in the predefined region and to communicate with one or more badges outside the predefined region,

wherein the first wireless beacon is able to communicate with the plural badges within the predefined region but is unable to communicate with the one or more badges outside the predefined region; and

determining the badges that are within the predefined region based on the first and second wireless beacons.

34. The article of claim 31, wherein the program code when executed cause the computer to further:

receive a parameter from each of the badges, the parameter indicating a confidence level that the respective badge has been worn continuously by a user.

35. The article of claim 31, wherein the program code when executed cause the computer to further:

re-determine the lowest clearance level as badges enter or leave the predefined region.

36. A system comprising:

storage to store sub-sets of information associated with corresponding plural clearance levels;

a first wireless beacon to communicate wirelessly with badges within a predefined region, each of the badges associated with one of the plural clearance levels;

a module to identify a lowest clearance level from among the clearance levels of the badges within the predefined region; and

software to provide access to one or more sub-sets of information in the storage having one or more clearance levels no higher than the identified lowest clearance level.

37. The system of claim 36, further comprising:

a second wireless beacon to communicate wirelessly with badges within the predefined region and at least one badge outside the predefined region,

wherein the first wireless beacon is unable to communicate with the at least one badge outside the predefined region,

the module to detect the badges that are within the predefined region based on the first and second wireless beacons.

38. The system of claim 37, wherein the second wireless beacon comprises a radio frequency beacon, and the first wireless beacon comprises an infrared beacon.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.